

**WHAT IS CLAIMED IS:**

1           1. A certificate validity authentication method wherein validity  
2 of a public key certificate issued by a certification authority which is  
3 different from a certification authority trusted by a terminal is  
4 authenticated in compliance with a request made by the terminal,  
5 comprising:

6           the path search step of executing a process in which, with any  
7 certification authority set as a start certification authority, an issue  
8 destination of a public key certificate issued by the start certification  
9 authority is checked, and subject to any certification authority included as  
10 the issue destination, an issue destination of a public key certificate issued  
11 by the issue-destination certification authority is further checked, the  
12 process being continued until all of the issue destinations of the public  
13 key certificates become terminals, thereby to search for paths which  
14 extend from said start certification authority to terminal admitting  
15 certification authorities having issued public key certificates to any  
16 terminals;

17           the path verification step of executing for each of the paths  
18 detected by said path search step, a process in which, with said start  
19 certification authority set at an upstream side, a signature of the public  
20 key certificate issued by the terminal admitting certification authority on  
21 the pertinent path is verified in the light of the public key certificate  
22 issued by the certification authority located directly upstream, and subject

23 to the verification having held good, a signature of the public key  
24 certificate issued by the terminal admitting certification authority located  
25 directly upstream is verified in the light of the public key certificate  
26 issued by the certification authority located directly upstream still further,  
27 the process being continued until said certification authority located  
28 directly upstream becomes said start certification authority, thereby to  
29 verify said paths;

30 the path registration step of registering in a database those of said  
31 paths whose verifications have held good by said path verification step;  
32 and

33 the validity authentication step of complying with the request of  
34 the terminal for authenticating the validity of the public key certificate  
35 issued by the terminal admitting certification authority which is different  
36 from the certification authority trusted by said terminal, to judge said  
37 validity of said public key certificate as having been authenticated when  
38 the path between said certification authority trusted by said terminal and  
39 said start certification authority and the path between the different  
40 terminal admitting certification authority and said start certification  
41 authority are held registered in the database.

1 2. A certificate validity authentication method according to  
2 Claim 1, wherein:

3 said path search step is performed periodically;

4 said path verification step is performed for a newest path searched  
5 for by said path search step; and

6 said path registration step updates registered contents of said

7 database to the newest path whose verification has held good by said path  
8 verification step.

1 3. A certificate validity authentication method according to  
2 Claim 1, further comprising:

3 the validity term examination step of examining for each of said  
4 paths registered in said database by said path registration step, validity  
5 terms of the public key certificates which the certification authorities on  
6 the pertinent path have issued to the certification authorities located  
7 directly downstream (to the terminals admitted by the terminal admitting  
8 certification authorities in a case where the issue origins are said terminal  
9 admitting certification authorities); and

10 the path re-verification step of obtaining any new public key  
11 certificate for an issue destination of the public key certificate whose  
12 validity term has been authenticated to have expired by said validity term  
13 examination step, from the issue origin of the term-expired public key  
14 certificate, and verifying at least a signature of the new public key  
15 certificate in the light of the public key certificate which has been issued  
16 by the certification authority located directly upstream of said issue  
17 origin;

18 wherein said path registration step deletes from said database the  
19 path including said issue origin and said issue destination of said public  
20 key certificate whose validity term has been authenticated to have expired  
21 by said validity term examination step, in either of a case where the  
22 verification of the signature of said new public key certificate has not held  
23 good at said path re-verification step and a case where said new public

24 key certificate has failed to be obtained.

1 4. A certificate validity authentication method according to  
2 Claim 1, further comprising:

3 the revocation information examination step of examining for each  
4 of said paths registered in said database by said path registration step,  
5 revocation information of the public key certificates which the  
6 certification authorities on the pertinent path have issued;

7 wherein said path registration step deletes from said database the  
8 path including said issue origin and said issue destination of any public  
9 key certificate which has been authenticated to have been revoked by said  
10 revocation information examination step.

1 5. A certificate validity authentication method according to  
2 Claim 1, wherein:

3 said validity authentication step complies with said request of said  
4 terminal for authenticating said validity of said public key certificate  
5 issued by said terminal admitting certification authority which is different  
6 from said certification authority trusted by said terminal, to judge said  
7 validity of said public key certificate as having failed to be authenticated  
8 in a case where a constraint to the effect that any certification authority  
9 located on said path between said certification authority trusted by said  
10 terminal and said start certification authority and said path between said  
11 different terminal admitting certification authority and said start  
12 certification authority is not trusted, is described in the public key  
13 certificate which any certification authority on the two paths has issued to

14 the certification authority located directly downstream (to the terminal  
15 admitted by the terminal admitting certification authority in a case where  
16 the issue origin is said terminal admitting certification authority) on the  
17 path where the issue-origin certification authority is located, even when  
18 said two paths are held registered in said database.

1 6. A certificate validity authentication method according to  
2 Claim 1, wherein:

3 said validity authentication step complies with said request of said  
4 terminal for authenticating said validity of said public key certificate  
5 issued by said terminal admitting certification authority which is different  
6 from said certification authority trusted by said terminal, to judge said  
7 validity of said public key certificate as having failed to be authenticated  
8 in a case where the total number of certification authorities located on  
9 said path between said certification authority trusted by said terminal and  
10 said start certification authority and said path between said different  
11 terminal admitting certification authority and said start certification  
12 authority exceeds a path length (the maximum allowable number of  
13 certification authorities located on the two paths) described in the public  
14 key certificate which any certification authority on said two paths has  
15 issued to the certification authority located directly downstream (to the  
16 terminal admitted by the terminal admitting certification authority in a  
17 case where the issue origin is said terminal admitting certification  
18 authority) on the path where the issue-origin certification authority is  
19 located, even when said two paths are held registered in said database.

1           7. A certificate validity authentication method according to  
2 Claim 1, wherein:

3           said validity authentication step complies with said request of said  
4 terminal for authenticating said validity of said public key certificate  
5 issued by said terminal admitting certification authority which is different  
6 from said certification authority trusted by said terminal, said request  
7 accompanying presentation of trustworthiness required of an electronic  
8 procedure intended by said terminal, to judge said validity of said public  
9 key certificate as having failed to be authenticated in a case where  
10 trustworthiness (policy) described in the public key certificate which any  
11 certification authority located on said path between said certification  
12 authority trusted by said terminal and said start certification authority  
13 and said path between said different terminal admitting certification  
14 authority and said start certification authority has issued to the  
15 certification authority located directly downstream (to the terminal  
16 admitted by the terminal admitting certification authority in a case where  
17 the issue origin is said terminal admitting certification authority) on the  
18 path where the issue-origin certification authority is located is lower than  
19 the trustworthiness required of the electronic procedure, even when the  
20 two paths are held registered in said database.

1           8. A certificate validity authentication method according to  
2 Claim 1, wherein said start certification authority is a bridge certification  
3 authority which performs cross-certification with respective root  
4 certification authorities of at least two security domains.

1           9. A certificate validity authentication apparatus wherein  
2 validity of a public key certificate issued by a certification authority which  
3 is different from a certification authority trusted by a terminal is  
4 authenticated in compliance with a request made by the terminal,  
5 comprising:

6           path search means for executing a process in which, with any  
7 certification authority set as a start certification authority, an issue  
8 destination of a public key certificate issued by the start certification  
9 authority is checked, and subject to any certification authority included as  
10 the issue destination, an issue destination of a public key certificate issued  
11 by the issue-destination certification authority is further checked, the  
12 process being continued until all of the issue destinations of the public  
13 key certificates become terminals, thereby to search for paths which  
14 extend from said start certification authority to terminal admitting  
15 certification authorities having issued public key certificates to any  
16 terminals;

17           path verification means for executing for each of the paths  
18 detected by said path search means, a process in which, with said start  
19 certification authority set at an upstream side, a signature of the public  
20 key certificate issued by the terminal admitting certification authority on  
21 the pertinent path is verified in the light of the public key certificate  
22 issued by the certification authority located directly upstream, and subject  
23 to the verification having held good, a signature of the public key  
24 certificate issued by the terminal admitting certification authority located  
25 directly upstream is verified in the light of the public key certificate  
26 issued by the certification authority located directly upstream still further,

27 the process being continued until said certification authority located  
28 directly upstream becomes said start certification authority, thereby to  
29 verify said paths;

30 path registration means for registering in a database those of said  
31 paths whose verifications have held good by said path verification means;  
32 and

33 validity authentication means complying with the request of the  
34 terminal for authenticating the validity of the public key certificate issued  
35 by the terminal admitting certification authority which is different from  
36 the certification authority trusted by said terminal, to judge said validity  
37 of said public key certificate as having been authenticated when the path  
38 between said certification authority trusted by said terminal and said start  
39 certification authority and the path between the different terminal  
40 admitting certification authority and said start certification authority are  
41 held registered in the database.

1 10. A storage medium which stores therein a program for  
2 authenticating validity of a public key certificate issued by a certification  
3 authority different from a certification authority trusted by a terminal, in  
4 compliance with a request made by the terminal;

5 the program being read and run by an electronic computer,  
6 thereby to build on the electronic computer:

7 path search means for executing a process in which, with any  
8 certification authority set as a start certification authority, an issue  
9 destination of a public key certificate issued by the start certification  
10 authority is checked, and subject to any certification authority included as



11 the issue destination, an issue destination of a public key certificate issued  
12 by the issue-destination certification authority is further checked, the  
13 process being continued until all of the issue destinations of the public  
14 key certificates become terminals, thereby to search for paths which  
15 extend from said start certification authority to terminal admitting  
16 certification authorities having issued public key certificates to any  
17 terminals;

18 path verification means for executing for each of the paths  
19 detected by said path search means, a process in which, with said start  
20 certification authority set at an upstream side, a signature of the public  
21 key certificate issued by the terminal admitting certification authority on  
22 the pertinent path is verified in the light of the public key certificate  
23 issued by the certification authority located directly upstream, and subject  
24 to the verification having held good, a signature of the public key  
25 certificate issued by the terminal admitting certification authority located  
26 directly upstream is verified in the light of the public key certificate  
27 issued by the certification authority located directly upstream still further,  
28 the process being continued until said certification authority located  
29 directly upstream becomes said start certification authority, thereby to  
30 verify said paths;

31 path registration means for registering in a database those of said  
32 paths whose verifications have held good by said path verification means;  
33 and

34 validity authentication means complying with the request of the  
35 terminal for authenticating the validity of the public key certificate issued  
36 by the terminal admitting certification authority which is different from

37 the certification authority trusted by said terminal, to judge said validity  
38 of said public key certificate as having been authenticated when the path  
39 between said certification authority trusted by said terminal and said start  
40 certification authority and the path between the different terminal  
41 admitting certification authority and said start certification authority are  
42 held registered in the database.